김해중
KBS 보도기술국

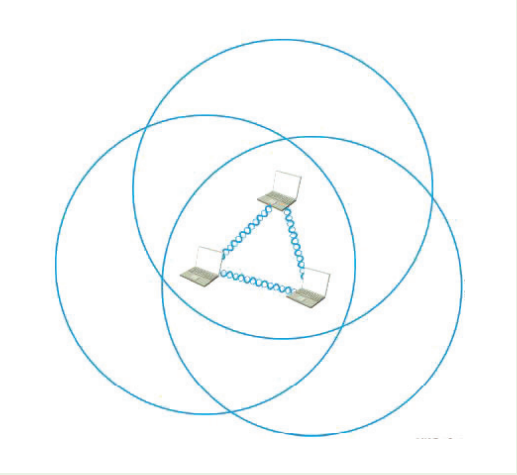
실무 네트워크 Design - 6 : WLAN(Wireless LAN) design

김해중 KBS 보도기술국

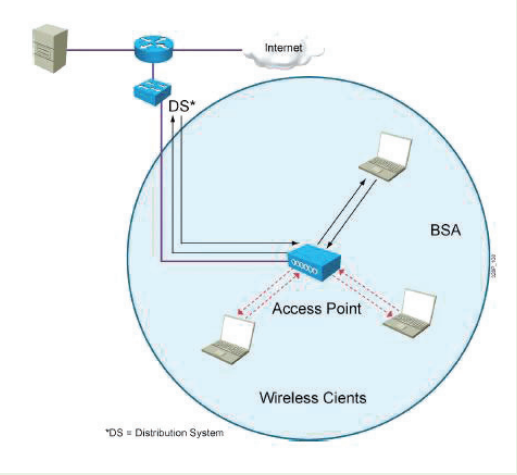
지난 시간까지는 유선 LAN을 다루었다면, 이제는 WLAN design에 대해서 설명하려 합니다. LAN을 기업, 개인에 의해 소유되는 network로 정의를 한다면, WLAN은 ISM(2.4Ghz, 5Ghz)를 사용하는 LAN으로 정의할 수 있습니다.
일반적으로 대부분의 책에서는 WLAN에서 사용하는 RF 기반기술(변조, 주파수, 802.11)과 다중접속기술인 CSMA/CA를 주로 설명하지만, 여기에서는 실제 WLAN이 유선 LAN과 어떻게 연동되는지를 다루려고 합니다. 초창기 기업 환경에서 무선 LAN 구축 시는 AP만을 사용한 Stand-alone 방식으로 구현했다면, 지금은 WLC(WLAN controller)를 이용하여 중앙 집중적으로 AP를 관리하는 방식으로 변경되고 있습니다.

WLAN Topology

유선 LAN의 topology에는 bus, ring, star가 존재하듯이, 무선 LAN의 topology는 AP(access Point)의 존재 여부에 따라서 Ad-hoc mode, infra-structure mode가 존재합니다. Ad-hoc mode는 AP 없이, 각 client 간에 직접 통신하는 방식이며, infra-structure 모드는 유선 LAN의 switch처럼 중앙에 AP가 존재하며, AP는 일반적으로 유선망(DS : distribution system)에 연결되어 있습니다. 일반적으로 WLAN이라고 하면 infra-structure mode를 의미합니다.
무선 LAN이라고 하지만 각 client(무선에서는 station이라고 함)에서 AP 구간까지만 사실 무선 구간이고, 나머지 구간은 유선입니다. 결국 WLAN은 client를 유선에서 무선으로 확장한 개념일 뿐입니다.

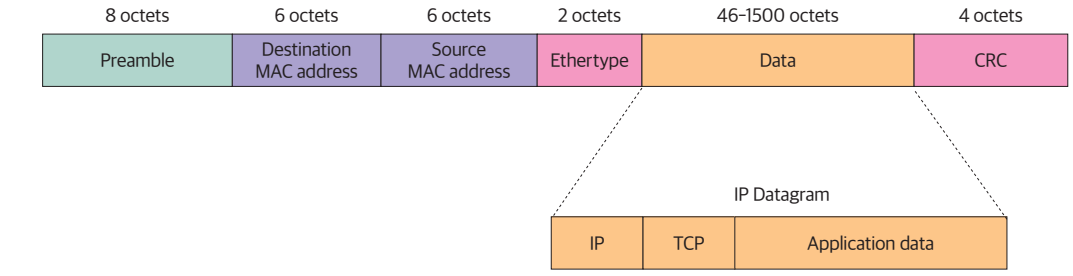


[그림 1] Ad-hoc mode

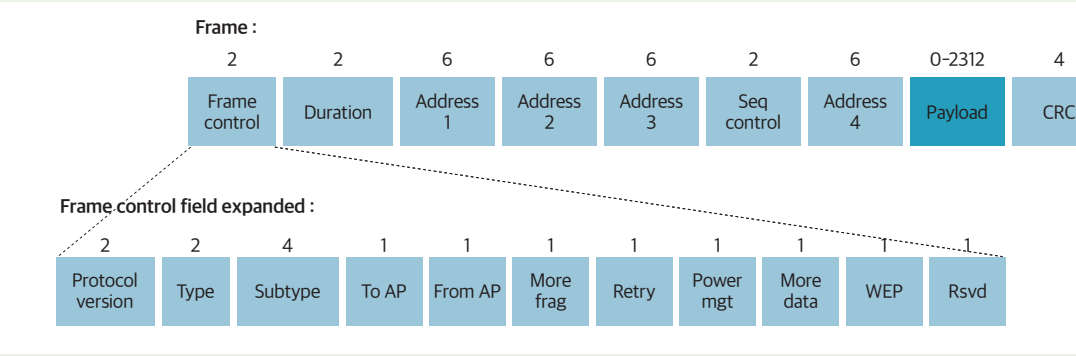


[그림 2] Infrastructure-mode

AP는 유선과 무선을 연결하면서, 수신한 무선 frame을 유선 frame으로 변경하는 역할을 하는데, 이것을 translation bridge로 표현합니다.



[그림 3] 유선 LAN의 frame 구조 : 2가지 주소(출발지, 목적지 주소)만을 가진다



[그림 4] WLAN frame 구조 : 4가지 주소로 표현을 해서 유선 frame보다 복잡하다

무선 frame은 [그림 4]와 같이 생겼는데, 유선일 때 frame 구조[그림 3]보다는 복잡하다는 것을 알 수 있습니다. 유선 LAN에서는 주소가(목적지, 출발지) 2가지만 존재하는데, 무선 LAN에서는 address(주소)가 무려 4개나 존재하며, frame도 복잡합니다. 이렇게 주소가 4개가 필요한 이유는, 유선 LAN과 달리 출발지와 목적지만을 기록하는 것이 아니라, 경유지(AP)의 주소도 같이 기록하기 때문입니다. 이때 무선 구간의 주소를 RA(receiver address), TA(transmitter address)라고 하며, 유선 구간의 출발지 주소를 SA(source address), 유선구간의 목적지 주소를 DA(Destination address)라고 합니다. WLAN에서 주소를 표현할 때는 TO_DS, From_DS도 같이 사용하는데, TO_DS란 AP에서 DS(일반적 유선이며, 무선중계 기능을 사용할 때만 무선임)로 패킷이 가는 것을 의미하며, From_DS는 DS에서 AP로 패킷이 가는 것을 의미합니다. To_DS, From_DS에 따라서 4가지 주소가 의미하는 바가 달라지는 점이 특이합니다. 이것에 대해서는 [표 1]에 정리되어 있습니다.

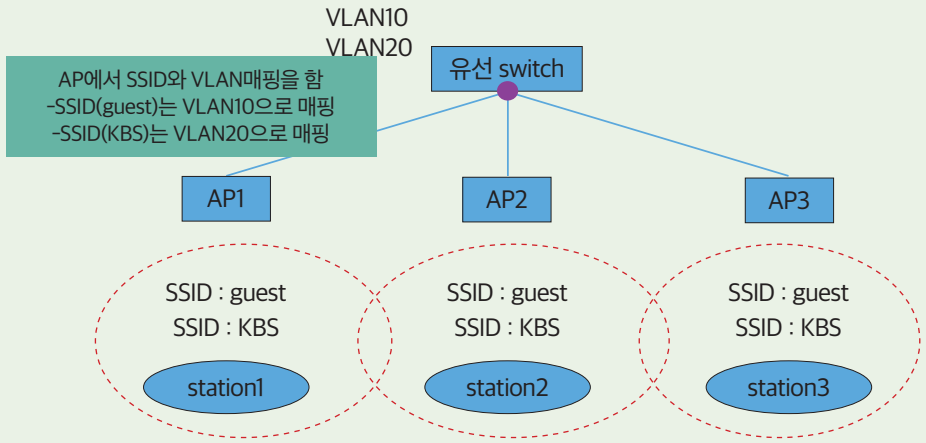
To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	RA/DA	TA/SA	BSSID	n/a
0	1	RA/DA	TA/BSSID	SA	n/a
1	0	RA/BSSID	TA/SA	DA	n/a
1	1	RA	TA	DA	SA

[표 1] WLAN에서 사용하는 주소 체계(4가지)

김해중
KBS 보도기술국

초창기의 Enterprise WLAN(Stand-alone 방식)

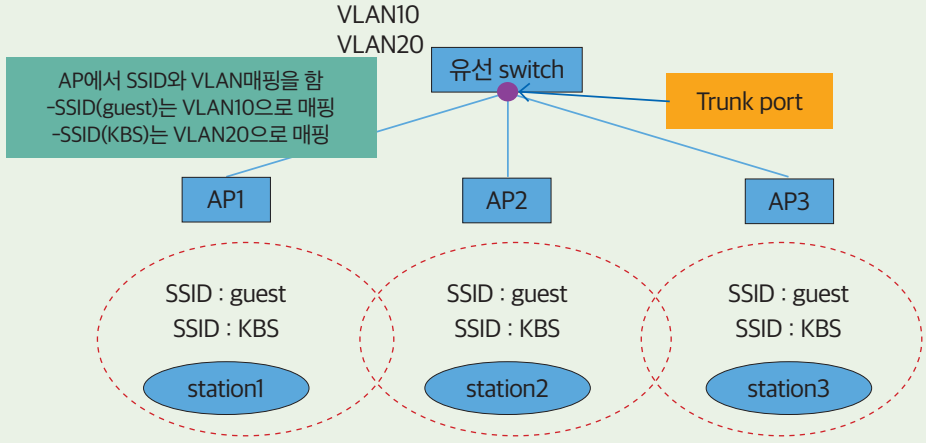
초창기에 기업에 구축된 대부분의 WLAN은, [그림 5]와 같이 일반적으로 구축되어 있는데 이 방식을 Stand-alone 방식이라고 합니다. 각 AP는 빨간색으로 표시된 RF coverage를 가지며, RF coverage 안의 station(client)에 서비스하도록 설계되었습니다. 조금씩 RF coverage를 겹치게 해두었는데, 이것은 WLAN의 roaming을 구현하기 위해서입니다. 참고로 그림을 편하게 그리기 위하여 1대의 유선 switch로 각 AP가 연결되게 그렸지만, 실제로 각 AP는 다른 유선 switch에 연결될 수도 있습니다.



[그림 5] 초창기 기업에 구축된 WLAN 구조

LAN에서는 VLAN을 통해서 각 client의 traffic을 구분했다면, WLAN에서는 SSID를 통해서 각각의 traffic을 구분합니다. [그림 5]을 보면 각 AP는 2개의 SSID(guest, kbs)를 전송하고 있으며, guest(SSID)는 guest 사용자를 위한 용도이고, kbs(SSID)는 kbs 직원을 위한 용도입니다. AP는 무선에서 분리된 traffic을 유선에서도 분리하기 위해 각 SSID를 각 VLAN에 매핑합니다. [그림 5]처럼 SSID(guest)의 traffic은 VLAN10, SSID(KBS)의 traffic은 VLAN20으로 매핑하여 traffic을 구분합니다.

이때 switch와 AP를 연결하는 port는 access, trunk port 중 어떤 것을 사용해야 할까요? [그림 6]처럼 여러 개의 VLAN(VLAN10, VLAN20)의 traffic이 들어오니 trunk로 설계를 합니다.

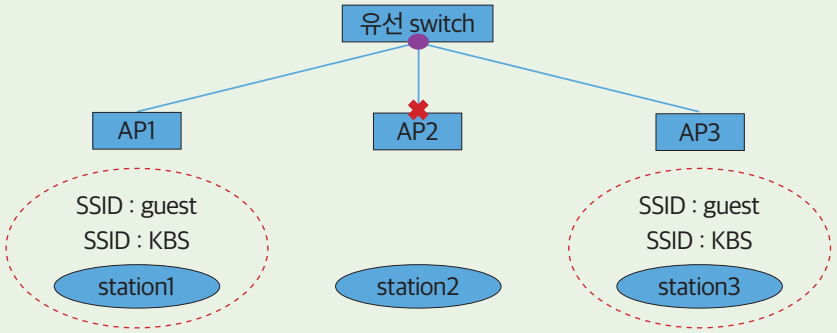


[그림 6] 유선 switch에서 AP를 연결하는 port는 Trunk로 설계합니다

Stand-alone 방식은 크게 3가지 문제점을 가지고 있습니다.

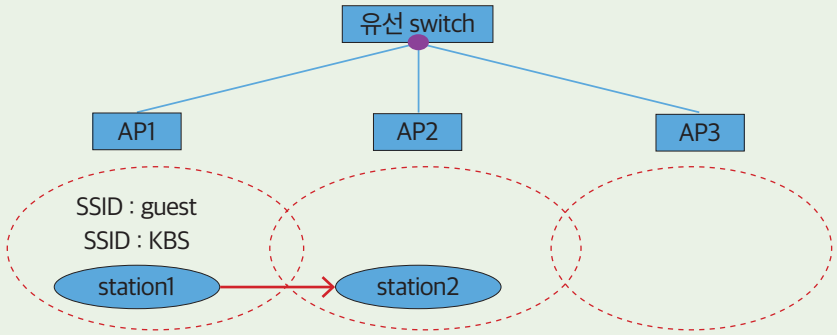
첫 번째는 관리가 불편합니다. 큰 회사는 AP를 수백 대 이상 설치하는데 장비마다 관리자는 SSID 세팅, RF 세팅, roaming 세팅을 하는 불편함이 존재합니다. Stand-alone 방식은 중앙 집중적인 관리를 할 수가 없기에, 관리자의 유지보수가 불편합니다.

두 번째는 AP 장애 발생 시, 동적으로 RF 대처가 힘들다는 것입니다. [그림 7]을 보면 AP2에 장애가 발생하면 해당 구역은 WLAN 전파가 도달하지 않아서, station2는 서비스를 받을 수 없습니다.



[그림 7] Stand-alone 방식은 AP 장애 발생 시 대처의 어려움이 존재함

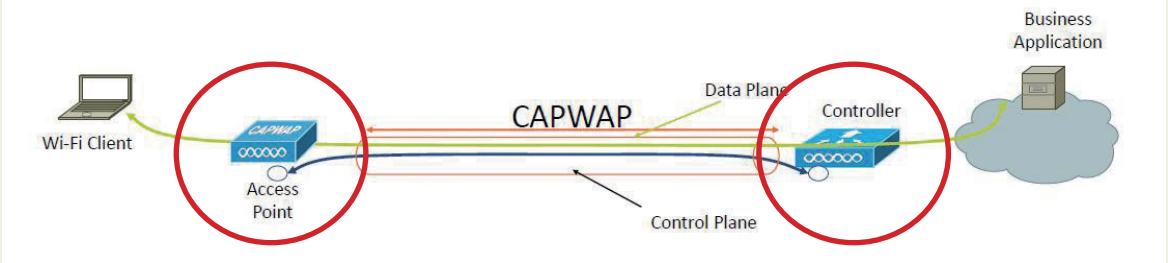
세 번째는 roaming 구현이 어렵습니다. [그림 8]처럼 station1이 AP1의 구역에서 AP2의 구역으로 이동 시, AP1에 기록된 station의 정보가 AP2로 기록이 넘어가야 됩니다. 이때 IAPP(Inter AP Protocol)을 사용하는데, 해당 protocol을 사용하더라도 seamless한 roaming 구현이 어렵고 복잡합니다.



[그림 8] Stand-alone 방식은 seamless roaming 구현이 어렵다

WLC(WLAN controller)를 이용한 방식

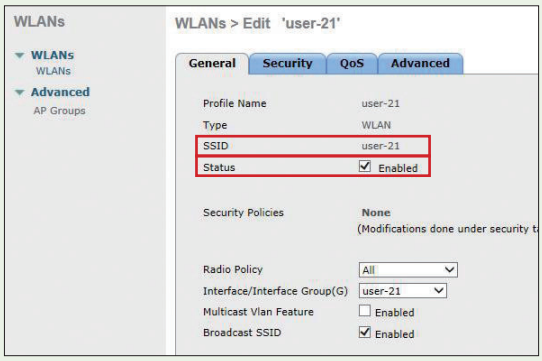
Stand-alone 방식의 문제점을 해결한 방식이 바로 [그림 9]처럼 WLAN controller를 이용한 방식입니다. 이 방식은 기존의 AP 역할 중 핵심 역할은 WLC(WLAN controller)로 넘기고, AP는 RF 전파만 방사해서, client가 WLAN에 접근하는 일만 합니다. 기존의 AP는 RF 관리, SSID 관리, Roaming 관리, QoS 관리를 했다면, 이제는 관리 기능은 모두 WLC에 넘겨주는데, 이때의 AP를 light AP라고 합니다. 기존의 AP의 역할에 비해서 업무가 많이 줄어들어서, 가벼워졌죠? 그래서 light AP라고 부릅니다.



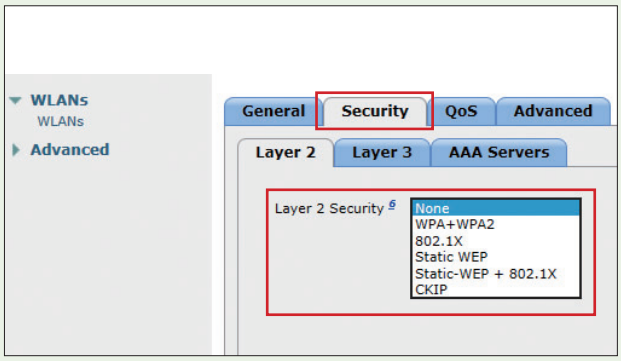
[그림 9] AP와 WLC 간에는 터널(CAPWAP, LWAPP)을 형성해서 통신한다

이렇게 되면 각 AP는 아무런 필요가 없으며, 모든 세팅은 WLC에서 하게 됩니다. 그러면 각 WLC에 세팅된 정보는 AP로 저절로 뿌려지게 됩니다.

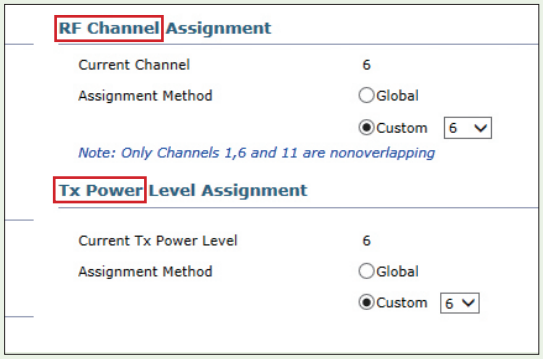
김해중
KBS 보도기술국



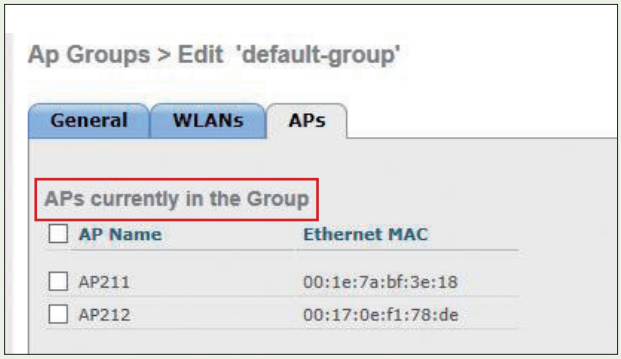
(a) WLC에서 SSID 세팅 환경



(b) WLC에서 SSID별 보안 정책을 결정한다



(c) WLC에서 RF channel과 TX power를 결정한다



(d) WLC에서 AP grouping이 가능하다

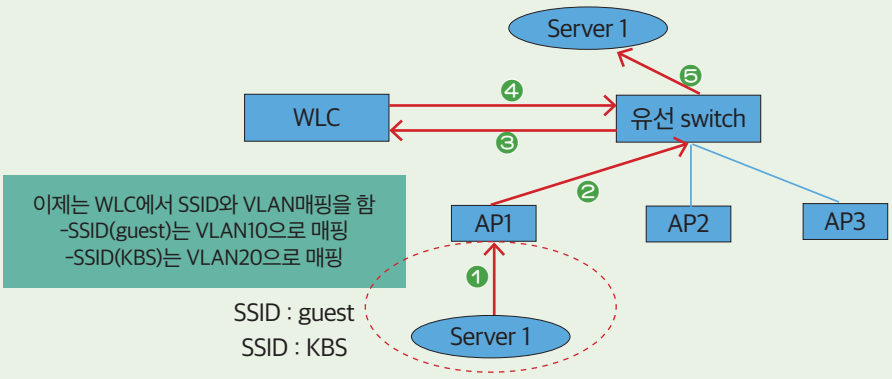
[그림 10] WLC(WLAN Controller)를 이용해서 중앙집중적인 관리를 한다

AP와 WLC 간에 통신을 위해서 tunnel을 형성하는데, 이때 사용하는 protocol로는 LWAPP, CAPWAP이 존재하는데, LWAPP는 cisco 전용 protocol이며, CAPWAP은 표준 기술입니다. [표 2]에 CAPWAP과 LWAPP을 비교를 해보았습니다. L2 mode란 AP와 WLC가 같은 subnet 상에 존재한다는 것이고, L3 mode는 AP와 WLC가 다른 subnet 상에 존재한다는 것입니다, LWAPP은 2가지 모드(L2, L3)를 모두 지원하지만, CAPWAP은 L3 mode만을 지원합니다.

	LWAPP	CAPWAP
암호화	control 패킷만 암호화	control/Data 모두 암호화
UDP Port	12222(Data),12223(control)	5246(control),Data(5247)
표준 여부	Cisco 기술(표준 아님)	표준 기술
mode	L2, L3 mode 지원	L3 mode만 지원

[표 2] 터널링 방식인 LWAPP와 CAPWAP 비교

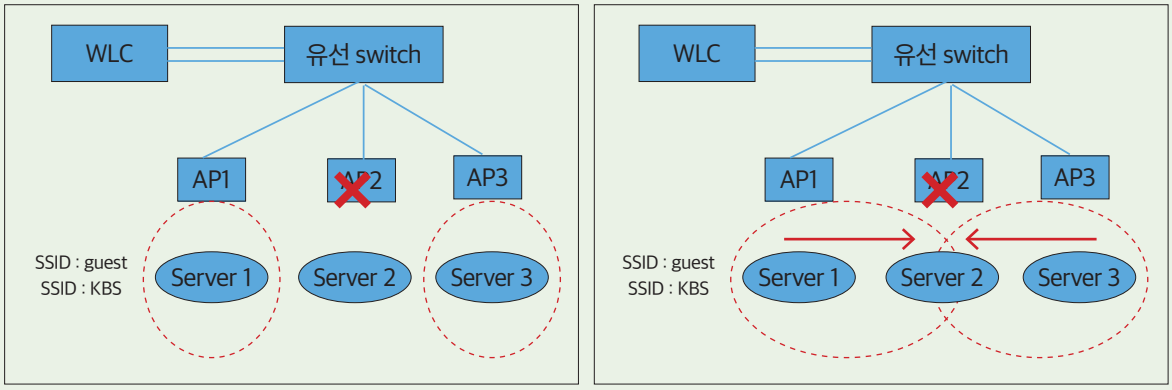
그러면 WLC를 사용했을 때의 traffic 흐름을 [그림 11]을 통해 살펴보도록 하겠습니다. 무선 client(station1)가 유선망에 있는 Server1과 통신한다고 가정을 하겠습니다. 최초에 station1은 RF 전파(SSID)를 뿌리는 AP1에 접속 후 Data를 보냅니다. AP1은 station에서 수신한 Data를 AP와 WLC 간에 만들어진 CAPWAP



[그림 11] 무선 client(Station 1)가 유선망에 있는 Server 1과 통신할 때의 traffic 흐름

터널을 통해서 WLC에 보내게 됩니다. WLC에 패킷이 도착하면 무선 SSID 값에 따라서 VLAN을 매핑하고, 무선 frame을 유선 frame으로 변경합니다. 이제 WLC는 원래 패킷의 목적지인 server1으로 보내게 됩니다. 굉장히 복잡해 보이지만, 출발지에서 보낸 모든 패킷이 중간의 경유지인 WLC를 통과하면서 목적지에 도착하게 되는 것입니다.

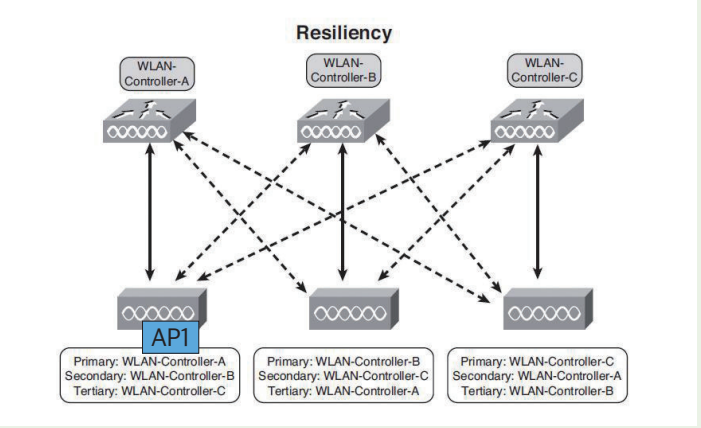
WLC 환경에서 1대의 AP에 장애가 발생했다고 가정해보겠습니다. AP에 장애가 발생해서 RF coverage hole이 발생하게 되면, [그림 12]과 같이 머리 역할을 하는 WLC에서는 동적으로 AP1과 AP3의 TX power를 증가시켜서 coverage hole을 제거합니다. 이 기능을 CHD(coverage hold detection)이라고 합니다.



(a) AP2에 장애가 발생 했을 때 (b) CHD 기능을 이용해 coverage hole을 제거함

[그림 12] AP 장애 시 WLC는 주변 AP의 power를 증가시켜서, RF hole을 제거한다

WLC 환경에서는 WLC가 중요한 역할을 하기에, 최소 WLC 2중화를 구현합니다. [그림 13]을 보면 AP1는 1순위로 WLC1로 모든 트래픽을 보내다가, WLC1에서 장애가 발생하면 WLC2로 보내고, WLC2까지 장애가 발생하면 WLC3로 보냅니다. 이렇게 AP마다 1순위, 2순위, 3순위 지정해서 평상시에는 Load-balancing을 구현하며, WLC 장애 발생 시는 fail-over 기능을 수행합니다.



[그림 13] 여러 대의 WLC를 사용해 장애를 대비한다

정리

개 념	특 징
Ad-hoc 모드	AP 없이 station 간에 직접 통신하는 topology
infra-structure 모드	AP를 사용하는 Topology이면서, 일반적으로 DS(Distribution system)에 연결되어 있다.
WLAN 주소 체계	유선 LAN과 달리 4가지 주소를 가지며, 중간에 경유지의 주소도 같이 기록한다.
Stand-alone 방식	WLC(controller) 없이, AP만을 사용하여 최초로 구현된 방식으로써, 중앙 집중적인 관리가 안 되는 문제점을 가지고 있다.
CAPWAP	AP와 WLC 간에 통신할 때 사용하는 터널링 프로토콜로, 표준 기술이며 L3 mode만을 지원한다.
LWAPP	AP와 WLC 간에 통신할 때 사용하는 터널링 프로토콜로, cisco전용 기술이며 L2/L3 mode를 지원한다.